

Cisco IOS 플랫폼에서 Errdisable 포트 상태 복구

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[Errdisable을 사용하는 플랫폼](#)

[Errdisable](#)

[Errdisable의 기능](#)

[Errdisable의 원인](#)

[포트가 Errdisable 상태인지 확인](#)

[Errdisable 상태의 이유 확인\(콘솔 메시지, 시스템 로그 및 show errdisabled recovery 명령\)](#)

[Errdisable 상태에서 포트 복구](#)

[근본 문제 해결](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 errdisable 상태를 설명하고, 이 상태에서 복구하는 방법을 설명하며, errdisabled 복구와 관련된 예시를 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

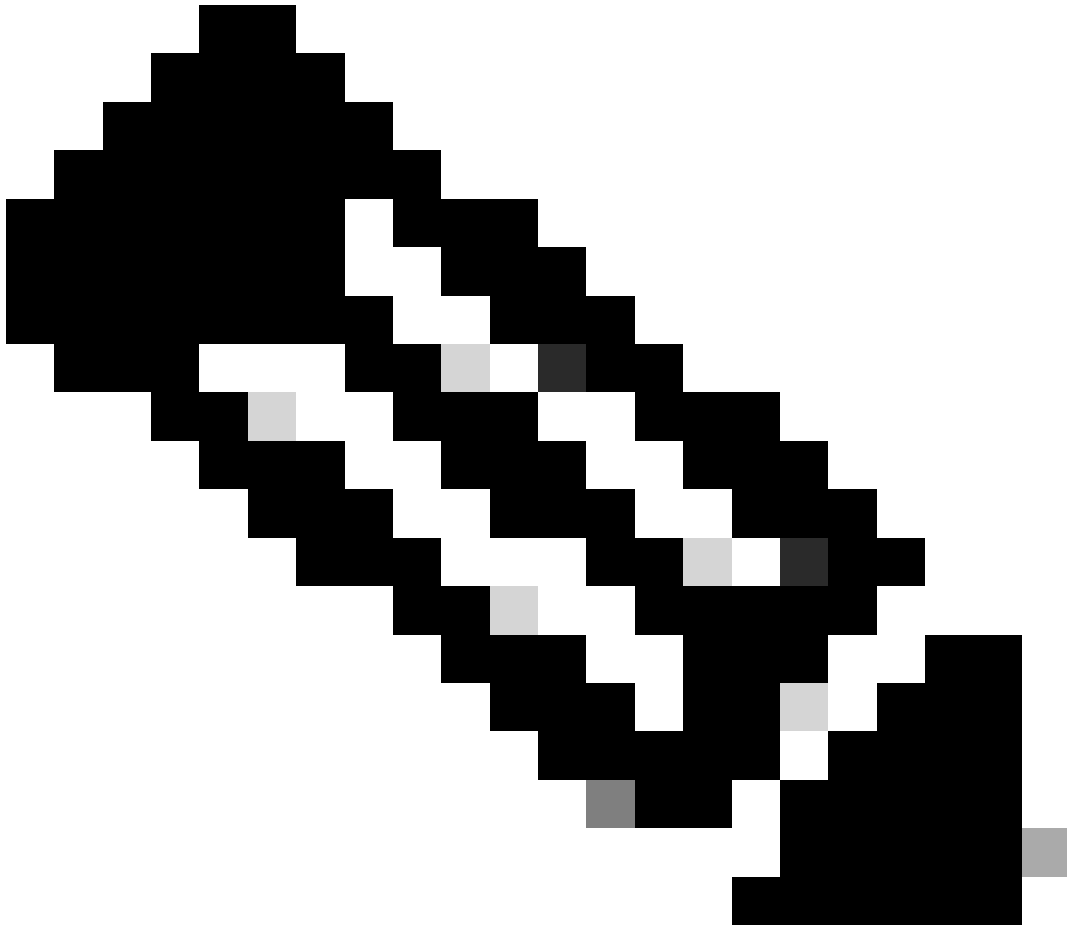
사용되는 구성 요소

이 문서의 예를 만들려면 실습 환경에서 컨피그레이션이 지워진 2개의 Cisco Catalyst 4500/6500 Series 스위치(또는 동급 스위치)가 필요합니다. 스위치는 Cisco IOS® Software를 실행해야 하며 각 스위치에는 EtherChannel 및 PortFast를 지원하는 두 개의 고속 이더넷 포트가 있어야 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 errdisable과 error disable이라는 용어를 서로 번갈아 사용합니다. 하나 이상의 스위치 포트가 error disable 상태 즉, 포트가 errdisable 상태임을 알고 [Cisco 기술 지원에 문의하는 고객이 자주 있습니다](#). 이러한 고객은 error disable가 발생한 이유와 포트를 어떻게 정상으로 복원할 수 있는지 알고자 합니다.



참고: err-disabled 포트 상태는 show interfaces interface_number status 명령의 출력에 표시됩니다.

Errdisable을 사용하는 플랫폼

errdisable 기능은 다음과 같은 Catalyst Switch에서 지원됩니다.

- Cisco IOS Software를 실행하는 Catalyst Switch:
 - 2900XL/3500XL

- 2940/2950/2960/2970
- 3550/3560/3560-E/3750/3750-E
- 3650/3850
- 4500/4503/4506/4507/4510/4500-X
- 6500/6503/6504/6506/6509
- 9200/9300/9400/9500

errdisable이 구현되는 방식은 소프트웨어 플랫폼에 따라 다릅니다. 이 문서에서는 Cisco IOS Software를 실행하는 스위치의 errdisable에 특히 중점을 둡니다.

Errdisable

Errdisable의 기능

컨피그레이션에서 포트가 활성 상태로 표시되지만 스위치의 소프트웨어가 포트에서 오류 상황을 감지하면 소프트웨어는 해당 포트를 종료합니다. 즉, 포트에서 발생한 오류 상태 때문에 스위치 운영 체제 소프트웨어에서 포트를 자동으로 비활성화한 것입니다.

포트가 error disable되면 사실상 종료되고 이 포트에서는 트래픽이 전송되거나 수신되지 않습니다. 포트 LED가 주황색으로 설정되어 있으며 show interfaces 명령을 실행하면 포트 상태가 err-disabled로 표시됩니다. 다음은 error disable 상태의 포트가 스위치의 CLI(command line interface)에 어떻게 표시되는지를 보여주는 예제입니다.

```
cat6knative#show interfaces gigabitethernet 4/1 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi4/1		err-disabled	100	full	1000	1000BaseSX

또는 오류 상태로 인해 인터페이스가 비활성화된 경우 콘솔과 시스템 로그에서 이와 유사한 메시지를 확인할 수 있습니다.

```
%SPANTREE-SP-2-BLOCK_BPDUGUARD:
```

```
Received BPDU on port GigabitEthernet4/1 with BPDU Guard enabled. Disabling port.
```

```
%PM-SP-4-ERR_DISABLE:
```

```
bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state
```

이 예제 메시지는 호스트 포트가 BPDU(bridge protocol data unit)를 수신하는 경우 표시됩니다. 실제 메시지는 오류 상태의 이유에 따라 달라집니다.

error disable 기능은 다음의 두 가지 목적으로 사용됩니다.

- 관리자가 포트 문제가 발생한 시기와 위치를 파악할 수 있게 해 줍니다.
- 이 포트가 모듈의 다른 포트(또는 전체 모듈)에 장애를 일으킬 가능성을 없애줍니다.

이러한 장애는 잘못된 포트가 버퍼를 독점하거나 포트 오류 메시지가 카드의 프로세스 간 통신을 독점할 때 발생할 수 있습니다. 이 경우 결국 심각한 네트워크 문제가 발생할 수 있습니다. error disable 기능은 이러한 상황을 방지하는 데 도움이 됩니다.

Errdisable의 원인

이 기능은 스위치가 포트에서 과도한 충돌 또는 낮은 충돌을 감지한 특정 충돌 상황을 처리하기 위해 처음 구현되었습니다. 과도한 충돌은 스위치가 충돌을 16개 연속으로 발견하여 프레임이 삭제될 때 발생합니다. 낮은 충돌은 전선의 모든 장치가 전선이 사용 중임을 인식하지 못했기 때문에 발생합니다. 이러한 유형의 오류가 발생하는 원인은 다음과 같습니다.


- 사양에 맞지 않는 케이블(길이가 너무 길거나 종류가 잘못되었거나 결함이 있는 경우)
- 불량 NIC(network interface card) 카드(물리적 문제 또는 드라이버 문제 포함)
- 포트 듀플렉스 컨피그레이션 오류

포트 듀플렉스 컨피그레이션 오류는 직접 연결된 두 디바이스(예: 스위치에 연결된 NIC) 간에 속도와 듀플렉스를 적절히 협상하는 데 실패하기 때문에 일반적인 오류 원인이 됩니다. LAN에서는 반이중 연결만 충돌을 일으킬 수 있습니다. 이더넷의 CSMA(carrier sense multiple access) 특성으로 인해 충돌이 소량의 트래픽을 초과하지 않는 한 하프 듀플렉스에서 충돌은 정상적인 현상입니다.

인터페이스가 errdisable 상태가 되는 데에는 여러 가지 이유가 있습니다. 예를 들면 다음과 같습니다.

- 듀플렉스 불일치
- 포트 채널 컨피그레이션 오류
- BPDU 가드 위반
- UDLD(UniDirectional Link Detection) 상태
- 낮은 충돌 감지
- 링크 플랩 감지
- 보안 위반
- PAgP(Port Aggregation Protocol) 플랩
- L2TP(Layer 2 Tunneling Protocol) 가드
- DHCP 스누핑 속도 제한

- 잘못된 GBIC/SFP(Small Form-Factor Pluggable) 모듈 또는 케이블
- ARP(Address Resolution Protocol) 검사
- 인라인 전원

 참고: Error-disable 탐지는 기본적으로 이러한 모든 이유로 활성화됩니다. error disable 감지를 비활성화하려면 no errdisable detect cause 명령을 사용하십시오. show errdisable detect 명령은 error-disable 감지 상태를 표시합니다.

포트가 Errdisable 상태인지 확인


show interfaces 명령을 실행하면 포트가 error-disable 상태인지 확인할 수 있습니다.

다음은 활성 포트의 예입니다.

```
cat6knative#show interfaces gigabitethernet 4/1 status
!--- Refer to show interfaces status for more information on the command.
Port    Name                Status      Vlan      Duplex  Speed Type
Gi4/1   Gi4/1                Connected   100       full    1000 1000BaseSX
```

다음은 동일한 포트가 error-disable 상태가 된 예입니다.

```
cat6knative#show interfaces gigabitethernet 4/1 status
!--- Refer to show interfaces status for more information on the command.
Port    Name                Status      Vlan      Duplex  Speed Type
Gi4/1   Gi4/1                err-disabled 100       full    1000 1000BaseSX
```

 참고: 포트가 error disabled(오류 비활성화) 상태인 경우, 포트와 연결된 전면 패널의 LED가 주황색으로 설정됩니다.

Errdisable 상태의 이유 확인(콘솔 메시지, 시스템 로그 및 show errdisabled recovery 명령)

포트를 error disable 상태로 설정할 경우 스위치는 포트를 비활성화한 이유를 설명하는 메시지를 콘솔에 전송합니다. 이 섹션의 예제에는 포트가 비활성화된 이유를 보여주는 샘플 메시지가 2개 나와 있습니다.

- 포트가 비활성화된 이유 중 하나는 PortFast BPDU 가드 기능 때문입니다.
- 다른 비활성화 이유는 EtherChannel 컨피그레이션 문제 때문입니다.

 참고: show log 명령을 실행하면 syslog에서도 이러한 메시지를 볼 수 있습니다.

다음은 샘플 메시지입니다.

```
%SPANTREE-SP-2-BLOCK_BPDUGUARD:
  Received BPDU on port GigabitEthernet4/1 with BPDU Guard enabled. Disabling port.

%PM-SP-4-ERR_DISABLE:
  bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state

%SPANTREE-2-CHNMISCFG: STP loop - channel 11/1-2 is disabled in vlan 1
```

errdisable recovery를 활성화한 경우 show errdisable recovery 명령을 실행하여 errdisable 상태의 이유를 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
cat6knative#show errdisable recovery
ErrDisable Reason    Timer Status
-----
udld                  Enabled
bpduguard             Enabled
security-violatio    Enabled
channel-misconfig    Enabled
pagp-flap            Enabled
dtp-flap              Enabled
link-flap            Enabled
l2ptguard            Enabled
psecure-violation    Enabled
gbic-invalid         Enabled
dhcp-rate-limit      Enabled
mac-limit            Enabled
unicast-flood        Enabled
arp-inspection       Enabled

Timer interval: 300 seconds

Interfaces that can be enabled at the next timeout:

Interface            Errdisable reason    Time left(sec)
-----
Fa2/4                bpduguard            273
```

Errdisable 상태에서 포트 복구

이 섹션에서는 포트가 error disable 상태인지 아는 방법과 해결책을 예제를 통해 살펴보고, 포트가 error disable 상태가 되는 다른 이유에 대해서도 간단히 이야기해 보겠습니다. errdisable 상태에서 포트를 복구하려면 먼저 근본 문제를 파악하고 수정한 후 포트를 다시 활성화하십시오. 근본 문제를 해결하기 전에 포트를 다시 활성화하면 포트가 다시 error-disable 상태가 됩니다.

근본 문제 해결

포트가 비활성화된 이유를 확인했다면 근본 문제를 해결하십시오. 해결 방법은 문제의 원인이 무엇인지에 따라 달라집니다. 종료될 수 있는 데는 여러 가지 원인이 있습니다. 이 섹션에서는 가장 일반적으로 눈에 띄는 원인 중 몇 가지를 설명합니다.

- EtherChannel 컨피그레이션 오류

EtherChannel이 작동하려면 관련된 포트의 컨피그레이션이 일관되어야 합니다. 즉, 포트의 VLAN, 트렁크 모드, 속도, 듀플렉스 등이 모두 동일해야 합니다. 스위치 내의 컨피그레이션 차이는 채널을 생성할 때 대부분 확인되고 보고됩니다. EtherChannel이 한 스위치에는 구성되고 다른 스위치에는 구성되지 않은 경우, EtherChannel이 구성되지 않은 쪽의 채널링된 포트가 스페닝 트리 프로세스에 의해 종료될 수 있습니다. EtherChannel의 on 모드는 채널링 전에 다른 측과 협상하기 위해 PAgP 패킷을 전송하지 않습니다. 다른 측이 채널링한다고 가정합니다. 또한 이 예제에서는 다른 스위치에 대한 EtherChannel을 켜지 않고 해당 포트를 채널링되지 않은 개별 포트에 남겨 둡니다. 다른 스위치를 EtherChannel을 켜지 않은 상태로 1분 정도 두면, EtherChannel이 켜진 스위치의 STP(Spanning Tree Protocol)는 루프가 발생했다고 생각합니다. 그러면 채널링 상태의 포트가 errdisable 상태가 됩니다.

이 예제에서는 루프가 감지되어 포트가 비활성화되었습니다. `show etherchannel summary` 명령의 출력에는 Number of channel-groups in use가 0으로 표시됩니다. 관련된 포트 중 하나를 보면 상태가 err-disabled임을 알 수 있습니다.

```
%SPANTREE-2-CHNL_MISCFG: Detected loop due to etherchannel misconfiguration of Gi4/1
```

```
cat6knative#show etherchannel summary
!--- Refer to show etherchannel for more information on the command.
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        u - unsuitable for bundling
Number of channel-groups in use: 0
Number of aggregators:          0

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
```

이 스위치에서 포트가 errdisable 상태가 되었기 때문에 EtherChannel이 해제되었습니다.

```
cat6knative#show interfaces gigabitethernet 4/1 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi4/1		err-disabled	100	full	1000	1000BaseSX

문제가 무엇인지 파악하기 위해 오류 메시지를 확인하십시오. 메시지를 통해 EtherChannel에 스페닝 트리 루프가 발생했음을 알 수 있습니다. 이 섹션에서 설명한 것처럼, 한 디바이스(이 경우에는 스위치)에서는 on 모드를 사용하여 수동으로 EtherChannel을 켜고(바람직하지 않음), 연결된 다른 디바이스(이 경우에는 다른 스위치)에서는 EtherChannel을 켜지 않은 경우 이 문제가 발생할 수 있습니다. 이러한 상황을 해결하는 한 가지 방법은 연결된 양쪽에서 모두 채널 모드를 바람직한 상태로 설정한 다음 포트를 다시 활성화하는 것입니다. 그러면 양쪽이 모두 채널에 동의하는 경우에만 각각 채널을 형성하게 됩니다. 채널에 동의하지 않더라도 양쪽은 정상 포트로서 계속 작동합니다.

```
cat6knative(config-terminal)#interface gigabitethernet 4/1
cat6knative(config-if)#channel-group 3 mode desirable non-silent
```

- 듀플렉스 불일치

일반적으로 듀플렉스 불일치는 속도와 듀플렉스를 적절히 자동 협상하지 못할 때 발생합니다. 동일한 LAN 세그먼트에서 다른 디바이스가 전송할 것이 없을 때까지 기다려야 하는 하프 듀플렉스 디바이스와 달리, 풀 듀플렉스 디바이스는 다른 디바이스에 관계없이 전송할 항목이 있을 때마다 전송합니다. 이러한 전송이 하프 듀플렉스 디바이스가 전송하는 동안 발생하면 하프 듀플렉스 디바이스는 이를 충돌(슬롯 시간 동안) 또는 늦은 충돌(슬롯 시간 이후)로 간주합니다. 풀 듀플렉스 측은 충돌을 예상하지 못하기 때문에 삭제된 패킷을 재전송해야 한다는 것을 인식하지 못합니다. 낮은 비율의 충돌은 하프 듀플렉스에서는 정상이지만 풀 듀플렉스에서는 정상이 아닙니다. 늦은 충돌을 많이 수신하는 스위치 포트는 일반적으로 듀플렉스 불일치 문제가 있음을 나타냅니다. 케이블 양쪽의 포트가 동일한 속도와 듀플렉스로 설정되어 있는지 확인하십시오. show interfaces interface_number 명령을 사용하여 Catalyst Switch 포트의 속도와 듀플렉스를 알 수 있습니다. CDP(Cisco Discovery Protocol)의 최신 버전은 포트가 error disable 상태에 놓이기 전에 듀플렉스 불일치를 경고할 수 있습니다.

자동 극성(autopolarity) 기능 같은 NIC의 설정으로 인해 듀플렉스 불일치 문제가 발생할 수도 있습니다. 의심스러우면 이 설정을 해제하십시오. 한 벤더의 NIC를 여러 개 사용 중이고 NIC에 모두 동일한 문제가 있는 것으로 보이면, 제조업체 웹사이트에서 릴리스 노트를 확인하고 사용 중인 드라이버가 최신 드라이버인지 확인하십시오.

늦은 충돌이 발생하는 기타 원인은 다음과 같습니다.

- 불량 NIC(컨피그레이션 문제와 물리적 문제 포함)
- 불량 케이블
- 너무 긴 케이블 세그먼트
- BPDU 포트 가드

PortFast를 사용하는 포트는 엔드 스테이션(예: 워크스테이션 또는 서버)에만 연결해야 하며 스페닝 트리 BPDU를 생성하는 디바이스(예: 스위치, 브리지 및 브리지)에는 연결해서는 안 됩니다. 스페닝 트리 PortFast 및 스페닝 트리 BPDU 가드가 활성화된 포트에서 스페닝 트리 BPDU를 수신하는 경우, 스위치는 잠재적 루프를 방지하기 위해 포트를 errdisable 모드에 둡니다. PortFast는 스위치에 있는 포트가 물리적 루프를 생성할 수 없다고 가정합니다. 따라서 PortFast는 해당 포트에 대한 초기 스페닝 트리 검사를 건너뛰고, 이로 인해 부팅 시 엔드 스테이션의 시간 초과가 방지됩니다. 네트워크 관리자는 PortFast를 신중하게 구현해야 합니다. PortFast가 활성화된 포트에서 BPDU 가드를

사용할 경우 LAN에서 루프를 방지할 수 있습니다.

이 예제에서는 BPDU 가드 기능을 설정하는 방법을 보여줍니다. 이 예제를 선택한 이유는 error disable 상황을 만드는 것이 쉽기 때문입니다.

```
cat6knative(config-if)#spanning-tree bpduguard enable  
!--- Refer to spanning-tree bpduguard for more information on the command.
```

이 예제에서는 Catalyst 6509 Switch가 다른 스위치(6509)에 연결되어 있습니다. 6500 스위치는 기본 스페닝 트리 설정을 사용하여 BPDU를 2초마다 전송합니다. 6509 스위치 포트에 PortFast가 활성화된 경우 BPDU 가드 기능은 이 포트에 들어오는 BPDU가 있는지 감시합니다. BPDU가 포트에 들어오면 즉, 엔드 디바이스가 아닌 디바이스가 해당 포트에서 감지되면 BPDU 기능은 스페닝 트리 루프의 가능성을 방지하기 위해 포트를 error disable 상태로 만듭니다.

```
cat6knative(config-if)#spanning-tree portfast enable  
!--- Refer to spanning-tree portfast \(interface configuration mode\) !--- for more information on the command.
```

Warning: Spanntree port fast start can only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops.

```
%PM-SP-4-ERR_DISABLE: bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state.
```

이 메시지는 PortFast 활성화 포트에서 스위치가 BPDU를 수신했고 이로 인해 포트 Gi4/1을 종료했음을 나타냅니다.

```
cat6knative#show interfaces gigabitethernet 4/1 status
```


Port	Name	Status	Vlan	Duplex	Speed	Type
Gi4/1		err-disabled	100	full	1000	1000BaseSX

이 포트는 잘못 연결된 포트이므로 PortFast 기능이 해제되어야 합니다. 연결이 잘못된 이유는 PortFast가 활성화되었고 스위치가 다른 스위치에 연결되었기 때문입니다. PortFast는 엔드 스테이션에 연결된 포트에만 사용된다는 점을 기억하십시오.

```
cat6knative(config-if)#spanning-tree portfast disable
```

- UDLD

UDLD 프로토콜은 광섬유 또는 구리 이더넷 케이블(예: 카테고리 5 케이블링)을 통해 연결된 디바이스에서 케이블의 물리적 컨피그레이션을 모니터링하고 단방향 링크 유무를 감지할 수 있게 합니다. 단방향 링크가 감지되면 UDLD는 해당 포트를 종료하고 사용자에게 이를 알립니다. 단방향 링크는 스페닝 트리 토폴로지 루프를 비롯한 여러 문제를 일으킬 수 있습니다.

 참고: UDLD는 인접 디바이스 간에 프로토콜 패킷을 교환합니다. 링크의 두 디바이스는 모두 UDLD를 지원하고 각 포트에 UDLD가 활성화되어야 합니다. 링크의 한 포트에만 UDLD를 활성화한 경우 UDLD로 구성된 엔드 디바이스가 errdisable 상태가 될 수도 있습니다.

UDLD에 대해 구성된 각 스위치 포트는 UDLD 프로토콜 패킷을 전송합니다. 이 패킷에는 포트 디바이스(또는 포트 ID)와 해당 포트에서 UDLD에 표시되는 네이버 디바이스(또는 포트 ID)가 포함되어 있습니다. 네이버 포트는 자체 디바이스, 또는 다른 쪽에서 수신되는 패킷의 포트 ID(에코)를 확인해야 합니다. 포트가 자체 디바이스 또는 일정 시간 동안 들어오는 UDLD 패킷의 포트 ID를 확인할 수 없는 경우 해당 링크는 단방향인 것으로 간주됩니다. 따라서 각 포트가 비활성화되고 다음과 유사한 메시지가 콘솔에 출력됩니다.

```
PM-SP-4-ERR_DISABLE: udld error detected on Gi4/1, putting Gi4/1 in err-disable state.
```

UDLD 작업, 구성 및 명령에 대한 자세한 내용은 [Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide](#) 문서를 참조하십시오.

- 링크 플랩 오류

링크 플랩은 인터페이스의 작동과 중단이 지속적으로 반복됨을 의미합니다. 인터페이스는 10초에 5회 넘게 플랩되면 errdisable 상태가 됩니다. 링크 플랩의 일반적인 원인은 불량 케이블, 듀플렉스 불일치 또는 불량 GBIC(Gigabit Interface Converter) 카드와 같은 레이어 1 문제입니다. 시스템 로그 서버에 전송된 메시지 또는 콘솔 메시지에서 포트 종료 이유가 나와 있는 메시지를 확인하십시오.

```
%PM-4-ERR_DISABLE: link-flap error detected on Gi4/1, putting Gi4/1 in err-disable state
```

플랩 값을 확인하려면 다음 명령을 실행하십시오.

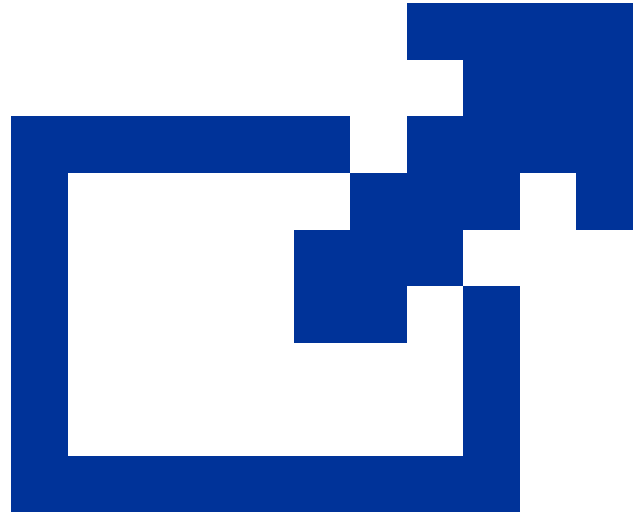
```
cat6knative#show errdisable flap-values
!--- Refer to show errdisable flap-values for more information on the command.
ErrDisable Reason      Flaps      Time (sec)
-----
pagp-flap              3          30
dtp-flap               3          30
link-flap              5          10
```

- 루프백 오류

keepalive 패킷이 keepalive를 전송한 포트에 다시 돌아가면 루프백 오류가 발생합니다. 스위치는 기본적으로 모든 인터페이스에서 keepalive를 전송합니다. 디바이스가 패킷을 소스 인터페이스로 다시 돌려보낼 수 있는데, 이는 스페닝 트리가 차단되지 않은 네트워크에 논리적 루프가 있을 때 보통 발생합니다. 소스 인터페이스는 전송한 keepalive 패킷을 수신하고 스위치는 인터페이스를 비활성화합니다(errdisable). 다음 메시지는 keepalive 패킷이 keepalive를 전송한 포트에 다시 돌아갔기 때문에 발생합니다.

```
%PM-4-ERR_DISABLE: loopback error detected on Gi4/1, putting Gi4/1 in err-disable state
```

기본적으로 keepalive는 Cisco IOS Software 릴리스 12.1EA 기반 소프트웨어의 모든 인터페이스에서 전송됩니다. Cisco IOS Software 릴리스 12.2SE 기반 소프트웨어 및 그 이상 버전에서 기본적으로 keepalive는 파이버 및 업링크 인터페이스에서 전송되지 않습니다. 자세한 내



용은 Cisco 버그 ID CSCea46385 (등록된 고객만 해당)를 참조하십시오.

권장되는 해결 방법은 keepalive를 비활성화하고 Cisco IOS Software 릴리스 12.2SE 이상으로 업그레이드하는 것입니다.

- 포트 보안 위반

포트의 인그레스 트래픽을 제한하기 위해 동적으로 학습된 고정 MAC 주소와 함께 포트 보안을 사용할 수 있습니다. 트래픽을 제한하기 위해 포트에 트래픽을 전송하도록 허용된 MAC 주소를 제한할 수 있습니다. 보안 위반이 발생할 때 스위치 포트를 error disable 상태가 되도록 구성하려면 다음 명령을 실행하십시오.

```
cat6native(config-if)#switchport port-security violation shutdown
```

보안 위반은 다음 두 가지 상황 중 하나에서 발생합니다.

- 보안 포트에서 보안 MAC 주소의 최대 개수에 도달하고 인그레스 트래픽의 소스 MAC 주소가 식별된 보안 MAC 주소와 다른 경우

이 경우, 포트 보안에서는 구성된 위반 모드를 적용합니다.

- 한 보안 포트에 구성되거나 학습된 보안 MAC 주소를 포함한 트래픽이 동일한 VLAN의 다른 보안 포트에 액세스하려는 경우

이 경우, 포트 보안에서는 종료 위반 모드를 적용합니다.

• L2pt 가드

레이어 2 PDU가 인바운드 에지 스위치의 터미널 포트 또는 액세스 포트에 진입하면, 스위치가 고객 PDU-대상 MAC 주소를 잘 알려진 Cisco 전용 멀티캐스트 주소(01-00-0c-cd-cd-d0)로 덮어씁니다. 802.1 Q 터널링이 활성화된 경우 패킷에는 이중 태그도 지정됩니다. 외부 태그는 고객 메트로 태그이고 내부 태그는 고객 VLAN 태그입니다. 코어 스위치는 내부 태그를 무시하고 동일한 메트로 VLAN의 모든 트렁크 포트에 패킷을 전달합니다. 아웃바운드 쪽의 에지 스위치가 올바른 레이어 2 프로토콜 및 MAC 주소 정보를 복원하고, 동일한 메트로 VLAN의 모든 터널 포트 또는 액세스 포트에 패킷을 전달합니다. 따라서 레이어 2 PDU는 그대로 유지되면서 서비스-공급자 인프라를 통해 고객 네트워크의 다른 쪽에 전달됩니다.

```
Switch(config)#interface gigabitethernet 0/7  
l2protocol-tunnel {cdp | vtp | stp}
```

인터페이스는 errdisabled 상태가 됩니다. 레이어 2 터널링이 활성화된 액세스 포트 또는 터널 포트로부터 캡슐화된 PDU(전용 대상 MAC 주소 포함)가 수신되는 경우 루프 방지를 위해 터널 포트가 종료됩니다. 포트는 프로토콜에 대해 구성된 종료 임계값에 도달하는 경우에도 종료됩니다. 포트를 수동으로 다시 활성화할 수 있습니다(shutdown, no shutdown 명령 시퀀스 실행). 또는 errdisable recovery가 활성화된 경우 지정된 시간 간격이 지나면 작업이 재시도됩니다.

errdisable 상태에서 인터페이스를 복구하려면 errdisable recovery cause l2ptguard 명령을 사용하여 포트를 다시 활성화합니다. 이 명령은 레이어 2 최대 속도 오류에서 복구 메커니즘을 구성하는 데 사용됩니다. 그러면 인터페이스가 비활성화된 상태에서 벗어나 다시 작업을 시도할 수 있습니다. 시간 간격도 설정할 수 있습니다. Errdisable 복구는 기본적으로 비활성화되어 있습니다. 활성화된 경우 기본 시간 간격은 300초입니다.

• 잘못된 SFP 케이블

Catalyst 3560 및 Catalyst 3750 스위치를 연결하고 SFP Interconnect 케이블을 사용할 때 포트는 %PHY-4-SFP_NOT_SUPPORTED 오류 메시지와 함께 errdisable 상태가 됩니다.

Cisco Catalyst 3560 SFP Interconnect 케이블(CAB-SFP-50CM=)은 Catalyst 3560 Series Switch 간에 낮은 비용의 point-to-point 기가비트 이더넷 연결을 제공합니다. 50cm(센티미터)

케이블은 SFP 트랜시버의 대안으로서 짧은 거리에서 SFP 포트를 통해 Catalyst 3560 Series 스위치를 상호 연결합니다. 모든 Cisco Catalyst 3560 Series Switch는 SFP Interconnect 케이블을 지원합니다.

Catalyst 3560 Switch가 Catalyst 3750 또는 기타 유형의 Catalyst Switch 모델에 연결된 경우에는 CAB-SFP-50CM= 케이블을 사용할 수 없습니다. 두 스위치를 CAB-SFP-50CM= 케이블 대신 두 디바이스에 SFP(GLC-T)가 있는 구리 케이블로 연결할 수 있습니다.

- 802.1X 보안 위반

```
DOT1X-SP-5-SECURITY_VIOLATION: Security violation on interface GigabitEthernet4/8,
New MAC address 0080.ad00.c2e4 is seen on the interface in Single host mode
%PM-SP-4-ERR_DISABLE: security-violation error detected on Gi4/8, putting Gi4/8 in err-disable sta
```

이 메시지는 지정된 인터페이스의 포트가 단일 호스트 모드로 구성되었음을 나타냅니다. 인터페이스에서 감지되는 새 호스트는 보안 위반으로 처리됩니다. 포트가 error disable 상태가 되었습니다.

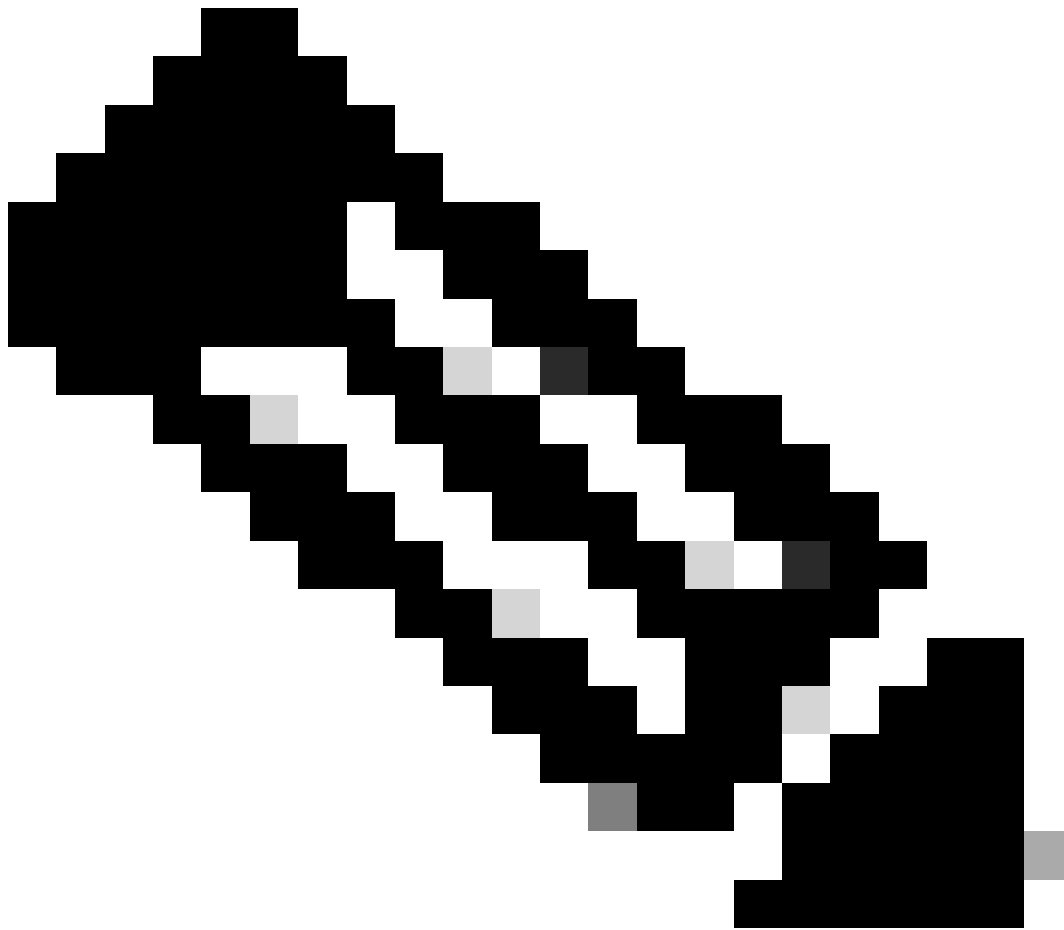
- 한 개의 호스트만 포트에 연결되어 있는지 확인하십시오. IP 폰 및 IP 폰 뒤에 있는 호스트에 연결해야 하는 경우 해당 switchport에 Multidomain Authentication 모드를 구성하십시오.
- MDA(Multidomain authentication) 모드를 사용할 경우, IP 폰 및 IP 폰 뒤에 있는 단일 호스트가 802.1 X, MAB(MAC authentication bypass) 또는 (호스트 전용) 웹 기반 인증을 통해 별개로 인증될 수 있습니다. 이 경우 Multidomain은 데이터와 음성이라는 두 개의 도메인을 말하고, 포트당 두 개의 MAC 주소만 허용됩니다. 스위치는 데이터 VLAN에 호스트를 두고, 음성 VLAN에 IP 폰을 둘 수 있는데, 이렇게 하면 두 개가 동일한 스위치 포트에 있는 것처럼 보입니다. 데이터 VLAN 할당은 인증 내 AAA 서버에서 수신된 VSA(vendor-specific attribute)에서 얻을 수 있습니다.
- 자세한 내용은 [Catalyst 4500 Series Switch Software Configuration Guide, 12.2\(50\)SG의 Multidomain Authentication Mode 섹션을](#) 참조하십시오.
- Errdisable 포트 다시 활성화

스위치에 errdisable recovery를 구성하지 않은 경우에는 근본 문제를 해결한 후에도 포트가 계속 비활성화됩니다. 이 경우에는 포트를 수동으로 다시 활성화해야 합니다. 포트를 수동으로 다시 활성화하려면 연결된 인터페이스에 shutdown 명령과 no shutdown 인터페이스 모드 명령을 차례대로 실행하십시오.

errdisable recovery 명령을 사용하면 지정된 시간 후에 포트를 자동으로 다시 활성화하는 오류 유형을 선택할 수 있습니다. show errdisable recovery 명령은 가능한 모든 조건에 대한 기본 error disable recovery 상태를 표시합니다.

```
cat6knative#show errdisable recovery ErrDisable Reason Timer Status -----
udld Disabled bpduguard Disabled security-violation Disabled channel-misconfig Disabled pagp-
flap Disabled dtp-flap Disabled link-flap Disabled l2ptguard Disabled psecure-violed gbic-invalid
```

Disabled dhcp-rate-limit Disabled mac-limit Disabled unicast-flood Disabled arp-inspection
Disabled Tired Timer interval: 300초 다음 시간 제한에서 활성화할 수 있는 인터페이스:



참고: 기본 시간 제한 간격은 300초이며, 기본적으로 시간 제한 기능은 비활성화되어 있습니다.

errdisable recovery를 켜고 errdisable 조건을 선택하려면 다음 명령을 실행하십시오.

- cat6native#errdisable recovery cause ? all enable timer to recover from arp-inspection arp inspection error disable state bpduguard 타이머 enable timer to recover from BPDU Guard error disable state channel-misconfig timer to recover from channel misconfig disable state dhcp-rate-limit 타이머 enable timer to recover from dhcp-rate-limit error disable state dtp-flap enable timer to recover from invalid GBIC error disable state l2ptguard enable timer to recover from l2protocol-tunnel error disable state link-flap timer enable timer to recover from link-flap error disable state mac-limit state pagp-flap enable timer to recover from pagp-error disable state psecure-violation state enable timer to recover from psecure violation state - violation 802.1x 위반에서 복구하기 위한 타이머 활성화 disable state udd에서 복구하기 위한

타이머 활성화 error disable state unicast-flood 유니캐스트 플러드 disable 상태에서 복구하기 위한 타이머 활성화.

이 예제에서는 BPDU 가드 errdisable recovery 조건을 활성화하는 방법을 보여줍니다.

cat6knative(Config)#errdisable 복구로 인해 bpduguard 발생

- 이 명령의 유용한 기능은 errdisable recovery를 활성화하면 포트가 error disable 상태가 된 일반적인 이유가 표시된다는 점입니다. 이 예제에서는 BPDU 가드 기능이 4개 포트 중 2개가 종료된 이유임을 알 수 있습니다.
- cat6knative#show errdisable recovery ErrDisable Reason Timer Status -----
---- uld Disabled bpduguard Enabled security-violation Disabled channel-misconfig Disabled pagp-flap Disabled dtp-flap Disabled link-flap Disabled l2ptguard Disabled psec psecure-violation Disabled gbic-invalid dhcp-rate-limit Disabled mac-limit Disabled unicast-flood Disabled arp-inspection Disable arp-inspection Timer interval: 300초 다음 시간 제한에서 활성화할 수 있는 인터페이스: Interface Errdisable Reason Time left(sec) -----
-- ----- Fa2/4 bpduguard 290
- errdisable recovery 조건 중 하나가 활성화되면 해당 조건의 포트는 300초 후에 다시 활성화됩니다. 기본값(300초)은 다음 명령을 실행하여 변경할 수도 있습니다.
- cat6knative(Config)#errdisable 복구 간격 timer_interval_in_seconds
- 다음 예제에서는 errdisable recovery 간격을 300초에서 400초로 변경합니다.
- cat6knative(Config)#errdisable 복구 간격 400

다음을 확인합니다.

- show version - 스위치에 사용된 소프트웨어 버전을 표시합니다.
- show interface interface interface_number status - 스위치 포트의 현재 상태를 표시합니다.
- show errdisable detect - errdisable 시간 초과 기능의 현재 설정을 표시하고, 포트가 현재 error disabled 상태인 경우 그 이유를 표시합니다.

문제 해결

- show interface status err-disabled - 어떤 로컬 포트가 errdisabled 상태에 있는지 표시합니다.
- show etherchannel summary - EtherChannel의 현재 상태를 표시합니다.
- show errdisable recovery - errdisable 상태에서 인터페이스가 활성화되는 시간을 표시합니다.
- show errdisable detect - errdisable 상태의 이유를 표시합니다.
- switchport 문제를 해결하는 방법에 대한 자세한 내용은 스위치 포트 [및 인터페이스 문제 해결을 참조하십시오](#).

관련 정보

- [Catalyst 6500/6000 Series 스위치의 하드웨어 및 일반 문제 해결](#)
- [루트 가드로 스페닝 트리 프로토콜 향상](#)
- [EtherChannel 불일치 탐지 이해](#)
- [스위치 포트 및 인터페이스 문제 해결](#)
- [LAN 제품 지원](#)
- [Technical Support - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.